2/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

011490013 **Image available**
WPI Acc No: 1997-467918/ **199743**
XRPX Acc No: N97-390315

Electronic shopping method for retail store - by subtracting price of goods, ordered and delivered to buyer from retail store, by credit card company after confirming validity of authentication information produced by buyer and porter

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9218896	A	19970819	JP 9622783	A	19960208	199743	B

Priority Applications (No Type Date): JP 9622783 A 19960208
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9218896	A		11	G06F-017/60	

Abstract (Basic): JP 9218896 A

The method involves producing the authentication information relating to a goods order sheet by a buyer during the order of goods. The authentication information and goods order sheet are transmitted to a retail store. The retail store confirms the validity of the authentication information from the buyer. Ordered goods of the buyer are passed to a porter and shipped by the personnel in the retail store after verifying the authentication information from the buyer.

When the buyer receives the ordered goods, the buyer demands for the goods receipt document and the porter confirms the validity of the authentication information in a duplicate copy. The goods receipt document and the confirmed authentication information in the duplicate copy are send by the retail store to a credit card company. The credit card company subtracts the price of ordered goods from the bank account of the buyer after confirming the validity of the authentication information from the buyer and porter.

ADVANTAGE - Prevents reduction of price of ordered goods from buyer bank account without passing goods. Safely transfers information until protected goods corresponding to buyer order is delivered.

Dwg.1/8

Title Terms: ELECTRONIC; SHOPPING; METHOD; RETAIL; STORAGE; SUBTRACT; PRICE ; GOODS; ORDER; DELIVER; BUY; RETAIL; STORAGE; CREDIT; CARD; COMPANY; AFTER; CONFIRM; VALID; AUTHENTICITY; INFORMATION; PRODUCE; BUY; PORTER
Derwent Class: P85; T01; T05; W01
International Patent Class (Main): G06F-017/60
International Patent Class (Additional): G09C-001/00; H04L-009/32
File Segment: EPI; EngPI

2/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05604096 **Image available**
ELECTRONIC SHOPPING METHOD AND DEVICE

PUB. NO.: 09-218896 [**JP 9218896** A]
PUBLISHED: August 19, 1997 (19970819)
INVENTOR(s): NISHIOKA GENJI
SASAKI RYOICHI
SUZAKI SEIICHI
UMEKI HISASHI
HANAOKA KAHORU

APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-022783 [JP 9622783]
FILED: February 08, 1996 (19960208)
INTL CLASS: [6] G06F-017/60; G09C-001/00; G09C-001/00; H04L-009/32
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)
JAPIO KEYWORD:R139 (INFORMATION PROCESSING -- Word Processors)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method for preventing illegality that a dishonest retail shop withdraws the information of a credit card from a purchaser and obtains a charge without delivering a product to the purchaser and making the purchaser safely recognize the carrying conditions of the product ordered by himself/ herself.

SOLUTION: The purchaser prepares authentication information in ordering the product and in receiving the product and a credit card company withdraws a product charge from the bank account of the purchaser after confirming the propriety of both of the authentication information. Also, the retail shop 300 arbitrarily prepares a ciphering key and a deciphering key intrinsic to the product in shipping the product ordered by the purchaser and delivers them respectively to a carrier 500 and the purchaser 200, the carrier 500 ciphers the information of the carrying conditions of the product by the ciphering key and stores it in a reliable server 700 and the purchaser 200 accesses the server 700 and views the carrying conditions of the product by using the deciphering key.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－218896

(43)公開日　平成９年(1997)８月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	17/60			Ｇ０６Ｆ	15/21	３４０Ａ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ
		６６０	7259－5Ｊ			６６０Ｂ
			7259－5Ｊ			６６０Ｇ
Ｈ０４Ｌ	9/32			Ｇ０６Ｆ	15/21	Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平8－22783

(22)出願日　平成８年(1996)２月８日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　佐々木　良一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

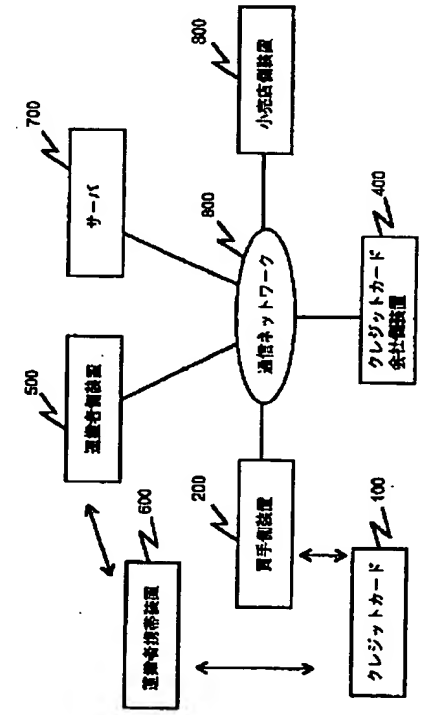
(54)【発明の名称】　電子ショッピング方法および装置

(57)【要約】

【課題】電子ショッピングシステムにおいて、不正な小売店が買手からクレジットカード１００の情報を引き出し、商品を買手に渡すことなく代金を得る不正を防止し、かつ、買手が自分の発注した商品の運搬状況を安全に知る方法を提供する。

【解決手段】買手は商品発注時と商品受け取り時に認証情報を作成し、クレジットカード会社は双方の認証情報の正当性を確かめた上で、買手の銀行口座から商品代金を引き落とす。また、小売店は買手の注文商品の発送時に商品固有の暗号化鍵と復号化鍵を任意に作成し、それぞれを運搬者および買手に渡し、運搬者は商品の運搬状況の情報を暗号化鍵で暗号化して信頼できるサーバ７００に格納し、買手はサーバ７００にアクセスし、復号化鍵を用いて商品の運搬状況を見る。

システム構成（図１）



1

【特許請求の範囲】

【請求項１】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手は商品注文時に商品注文書Ｐに関する認証情報Ｉ１を作成し、ＰとＩ１を小売店に送り、

小売店は認証情報Ｉ１の正当性を確かめた後、買手の注文した該商品を運搬者に渡し発送し、さらにＰとＩ１をクレジットカード会社に送り、

買手は運搬者から該商品を受け取った際に、商品受取書Ｒに対して認証情報Ｉ２を作成し、Ｉ２を運搬者に渡し、

運搬者はＩ２の正当性を確かめた後、ＲとＩ２を（小売店経由で）クレジットカード会社に送信し、

クレジットカード会社はＩ１とＩ２の正当性を確かめた後、該商品代金を買手の銀行口座から引き落とすことを特徴とする電子ショッピング方法。

【請求項２】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手のクレジットカードには買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が搭載されており、クレジットカード会社は公開鍵（ｅ，ｎ）を管理しており、

買手は、商品注文時に商品注文書Ｐに対してクレジットカード内の秘密鍵ｄを用いて署名Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成し、ＰとＳ１を小売店に送り、

小売店は、クレジットカード会社に買手の公開鍵（ｅ，ｎ）を問い合わせて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ１の認証を行った後、買手の注文した該商品を運搬者に渡し発送し、さらにＰとＳ１をクレジットカード会社に送信し、

買手は運搬者から該商品を受け取った際に、クレジットカード内の秘密鍵ｄを用いて商品受取書Ｒに対して、

Ｓ２＝ｅｘｐ（ｈ（Ｒ），ｄ）　ｍｏｄ　ｎ，

にて、署名Ｓ２を作成し、Ｓ２を運搬者に渡し、

運搬者は、買手のクレジットカードから出力された公開鍵（ｅ，ｎ）を用いて、

ｈ（Ｒ）　ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ２の認証を行った後、ＲとＳ２を（小売店経由で）クレジットカード会社に送信し、

クレジットカード会社は、クレジットカード会社に保管

2

されている買手の公開鍵（ｅ，ｎ）を用いて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

ｈ（Ｒ）　ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより、Ｓ１とＳ２の認証を行った後、該商品代金を買手の銀行口座から引き落とすことを特徴とする電子ショッピング方法。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ　１（ｍｏｄ　Ｎ）（Ｎはｐ－１とｑ－１の最小公倍数）であり、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表し、ｈは公開されたハッシュ関数を表す。

【請求項３】請求項１および請求項２において、

商品受取書および受取書に対する買手の署名のコピーのデータを買手のクレジットカードまたは他の記憶媒体に記録し、買手は該データを保管することを特徴とする電子ショッピング方法。

【請求項４】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

小売店は買手の注文した商品発送時に該商品に対して識別情報Ｉと固有の鍵情報（暗号化鍵と復号化鍵）を設定し、小売店は識別情報Ｉと該復号化鍵を買手に送信し、

買手の注文した該商品と識別情報Ｉと該暗号化鍵を運搬者に渡し、

運搬者は該商品の運搬状況の情報を該暗号化鍵で暗号化した暗号化データを信頼できるサーバに格納し、

買手は該商品の運搬状況を知ることを目的に該サーバにアクセスし、該商品の識別情報Ｉから該暗号化データを検索し、該暗号化データを該復号化鍵で復号化することを特徴とする電子ショッピング方法。

【請求項５】買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピング方法において、

買手のクレジットカードには買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が搭載されており、クレジットカード会社は公開鍵（ｅ，ｎ）を管理しており、

買手は、商品注文時に商品注文書Ｐに対してクレジットカード内の秘密鍵ｄを用いて署名Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成し、ＰとＳ１を小売店に送り、

小売店は、クレジットカード会社に買手の公開鍵（ｅ，ｎ）を問い合わせて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ１の認証を行った後、買手からの該注文商品に対して識別情報Ｉと固有の鍵情報Ｋ（共通鍵暗号の鍵）を設定し、小売店は該商品と識別情

報Ｉと鍵情報Ｋを運搬者に渡し、さらに買手の公開鍵（ｅ，ｎ）を用いて、

Ｗ＝ｅｘｐ（Ｋ，ｅ）　ｍｏｄ　ｎ，

にて鍵Ｋを暗号化して、ＷとＩを買手に送信し、

運搬者は該商品の運搬状況の情報Ｓを鍵Ｋで、

Ｅ＝Ｅ（Ｓ：Ｋ），

にて暗号化して、信頼できるサーバに格納し、

買手は小売店から送られてきた暗号文Ｗから、クレジットカード内の秘密鍵ｄと公開鍵（ｅ，ｎ）を用いて、

Ｋ＝ｅｘｐ（Ｗ，ｄ）　ｍｏｄ　ｎ，

にて、鍵Ｋを復号化し、さらに該商品の運搬状況を知ることを目的に該サーバにアクセスし、該商品の識別情報Ｉから該暗号化データＥを検索し、鍵Ｋを用いて、

Ｓ＝Ｄ（Ｅ：Ｋ），

にて、Ｓを復号化することを特徴とする電子ショッピング方法。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ　１（ｍｏｄ　Ｎ）（Ｎはｐ－１とｑ－１の最小公倍数）であり、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表し、ｈは公開されたハッシュ関数を表わし、Ｅ（Ｐ：Ｋ），Ｄ（Ｐ：Ｋ）はそれぞれ文書Ｐを鍵Ｋで暗号化、復号化した結果を表す。

【請求項６】請求項２から請求項６のいずれかにおいて、

クレジットカード会社は、買手の手元に商品が届けられた日時から商品返品有効期間を経た後、買手の銀行口座から代金を引き落とすことを特徴とする電子ショッピング方法。

【請求項７】請求項１または２において、買手が商品受け取り時に受取書に対して署名を作成するときに用いられる運搬者が所持する携帯可能な装置であって、

受取書を表示する表示手段と、買手がクレジットカード内の秘密鍵を用いて作成した署名文を記憶する記憶手段と、該署名の正当性を確かめる検証手段を備えたことを特徴とする携帯可能な装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、買手が通信ネットワークを介して商品発注を行う電子ショッピングシステムに関する。

【０００２】

【従来の技術】一般にクレジットカードを用いて通信販売を行う場合、買手は商品発注の際に買手のクレジットカードの会社名、クレジットカード番号、有効期限、等の情報を小売店に知らせ、小売店はクレジットカード会社に対して代金請求を行ない、クレジット会社は後日買手の銀行口座から商品の代金引き落としを行っている。

【０００３】

【発明が解決しようとする課題】しかし、この方法だと、不正な小売店が買手からクレジットカードの情報を引き出し、商品発送を行わないで代金のみを得るような不正が考えられる。

【０００４】また、今日、インターネットを利用して、海外の通販業者に対して手軽にメールオーダーを行えるようになりつつある。しかし、国内と違って、買手の手元に商品が届くまでには相当の日数がかかり、買手は自分が注文した商品の状況（商品が現在どこにあって、いつ買手の手元に届くか等）が分かると便利である。

【０００５】そこで、本発明の主目的は、（１）不正な小売店が買手からクレジットカードの情報を引き出し、商品を買手に渡すことなく代金を得る不正を防止する、（２）買手は、自分の発注した商品が買手の手元に届くまでの運送状況を買手のプライバシーを保護し安全に知ることができる、という特徴を有する電子ショッピングシステムを提供するものである。

【０００６】

【課題を解決するための手段】上記目的（１）を達成するために、本発明は、買手が商品発注時に作成した認証情報と商品受け取り時に作成した認証情報の双方の正当性を確かめた上で、クレジットカード会社は買手の銀行口座から代金を引き落とすようにしたことを特徴とする。

【０００７】具体的には、買手のクレジットカードには買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が搭載されており、クレジットカード会社は公開鍵（ｅ，ｎ）を管理しており、買手は、商品注文時に商品注文書Ｐに対してクレジットカード内の秘密鍵ｄを用いて署名Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成し、ＰとＳ１を小売店に送る。

【０００８】小売店は、クレジットカード会社に買手の公開鍵（ｅ，ｎ）を問い合わせて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ１の認証を行った後、買手の注文した商品を運搬者に渡し発送し、さらにＰとＳ１をクレジットカード会社に送信する。

【０００９】買手は運搬者から商品を受け取った際に、クレジットカード内の秘密鍵ｄを用いて商品受取書Ｒに対して、

Ｓ２＝ｅｘｐ（ｈ（Ｒ），ｄ）　ｍｏｄ　ｎ，

にて、署名Ｓ２を作成し、Ｓ２を運搬者に渡す。

【００１０】運搬者は、買手のクレジットカードから出力された公開鍵（ｅ，ｎ）を用いて、

ｈ（Ｒ）　ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ２の認証を行った後、ＲとＳ２を（小売店経由で）クレジットカード会社に送信する。

【００１１】クレジットカード会社は、クレジットカード会社に保管されている買手の公開鍵（ｅ，ｎ）を用いて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

ｈ（Ｒ）　ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより、Ｓ１とＳ２の認証を行った後、該商品代金を買手の銀行口座から引き落とす。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ　１（ｍｏｄＮ）（Ｎはｐ－１とｑ－１の最小公倍数）であり、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表し、ｈは公開されたハッシュ関数を表す。

【００１２】また、上記目的（１）、（２）を達成するために、本発明は、小売店が注文商品を発送する際に作成した商品固有の暗号化鍵と復号化鍵をそれぞれ運搬者と買手に渡し、運搬者は買手の注文した商品の運搬状況の情報を暗号化鍵で暗号化して信頼できるサーバに格納し、買手はサーバにアクセスし、復号化鍵を用いて運搬状況の情報を復号化して、自分の注文した商品の運搬状況を知る。

【００１３】具体的には、買手のクレジットカードには買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が搭載されており、クレジットカード会社は公開鍵（ｅ，ｎ）を管理しており、買手は、商品注文時に商品注文書Ｐに対してクレジットカード内の秘密鍵ｄを用いて署名Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成し、ＰとＳ１を小売店に送る。

【００１４】小売店は、クレジットカード会社に買手の公開鍵（ｅ，ｎ）を問い合わせて、

ｈ（Ｐ）　ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

を確かめることにより署名Ｓ１の認証を行った後、買手からの注文商品に対して識別情報Ｉと固有の鍵情報Ｋ（共通鍵暗号の鍵）を設定し、小売店は商品と識別情報Ｉと鍵情報Ｋを運搬者に渡し、さらに買手の公開鍵（ｅ，ｎ）を用いて、

Ｗ＝ｅｘｐ（Ｋ，ｅ）　ｍｏｄ　ｎ，

にて鍵Ｋを暗号化して、ＷとＩを買手に送信する。

【００１５】運搬者は商品の運搬状況の情報Ｓを鍵Ｋで、

Ｅ＝Ｅ（Ｓ：Ｋ），

にて暗号化して、信頼できるサーバに格納する。

【００１６】買手は小売店から送られてきたＷから、クレジットカード内の秘密鍵ｄと公開鍵（ｅ，ｎ）を用いて、

Ｋ＝ｅｘｐ（Ｗ，ｄ）　ｍｏｄ　ｎ，

にて、鍵Ｋを復号化し、さらに該商品の運搬状況を知ることを目的に該サーバにアクセスし、該商品の識別情報Ｉから該暗号化データＥを検索し、鍵Ｋを用いて、

Ｓ＝Ｄ（Ｅ：Ｋ），

にて、Ｓを復号化する。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ　１（ｍｏｄＮ）（Ｎはｐ－１とｑ－１の最小公倍数）であり、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表し、ｈは公開されたハッシュ関数を表わし、Ｅ（Ｐ：Ｋ），Ｄ（Ｐ：Ｋ）はそれぞれ文書Ｐを鍵Ｋで暗号化、復号化した結果を表す。

【００１７】なお、共通鍵を用いる暗号方式では、暗号化鍵と復号化鍵が同一で、それぞれを秘密に管理する必要がある。これに対して、公開鍵暗号方式は、暗号化鍵と復号化鍵とが相異なっており、暗号化鍵は公開し、復号化鍵は秘密にする。これにより、誰でも暗号文をつくることができ、復号化鍵を持つ者だけが復号を行える。このことから、公開鍵暗号方式では暗号化鍵のことを公開鍵と呼び、復号化鍵を秘密鍵と呼ぶ。但し、デジタル署名においては、秘密鍵を用いて署名作成を行い、公開鍵を用いて署名検証を行う。すなわち、署名鍵を知る者のみ署名を作成でき、その署名が正当なものであるかどうかは誰でもが確かめることができるようにするものである。

【００１８】ハッシュ関数とは、データを圧縮する関数であり、従来提案されているハッシュ関数（例えばＭＤ２，ＭＤ５等）のうち適当なものを使用すればよい。圧縮されたデータが元に復元できなくてもよい。なお、ハッシュ関数の詳細については、例えば、岡本栄司著、「暗号理論入門」、共立出版（１９９３）、第１３８～１４１頁に記載されている。

【００１９】また、公開鍵暗号については、前述の「暗号理論入門」の第８８～９１頁に記載されている。

【００２０】本発明に係る電子ショッピング方法によれば、クレジットカード会社は商品発注時の署名と商品受け取り時の署名の双方の正当性を確かめた後、買手の銀行口座より代金を引き落とす。このため、不正な小売店が商品を発送せずに代金のみを得る不正を防止することができる。また、買手の注文した商品の運搬状況の情報を暗号化して信頼できるサーバに格納しているため、不正な小売店が商品発送を行わなかった場合、買手はこれを検出することができ、さらに第３者から買手のプライバシーを保護し、買手は商品が手元に届くまでの運搬状況の情報を得ることができる。

【００２１】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態について詳しく説明する。

【００２２】図１は、本発明の実施の形態１及び２のシステム構成を示す図である。このシステムは、クレジットカード１００と買手側装置２００と小売店側装置３００とクレジットカード会社側装置４００と運搬者側装置５００と運搬者携帯装置６００とサーバ７００から構成されている。これらは、いずれもコンピュータにより実現される。買手側装置２００と小売店側装置３００とクレジットカード会社側装置４００と運搬者側装置５００とサーバ７００は通信ネットワーク８００を介して接続されている。運搬者携帯装置６００および買手側装置２００は、後述するように、クレジットカード１００とのインタフェースを有する。

【００２３】図２はクレジットカード１００の内部構成を示す。クレジットカード１００は、メモリ１０１、署名作成装置１０２、暗復号化装置（公開鍵暗号）１０

３、を備えている。

【００２４】図３は買手側装置２００の内部構成を示す。買手側装置２００は、クレジットカード読み取り装置２０１、文書作成装置２０２、ハッシュ計算装置２０３、暗復号化装置（共通鍵暗号）２０４、メモリ２０５、通信装置２０６、を備えている。

【００２５】図４は小売店側装置３００の内部構成を示す。小売店側装置３００は、ハッシュ計算装置３０１、署名検証装置３０２、暗復号化装置（公開鍵暗号）３０３、鍵生成装置３０４、通信装置３０５、を備えている。

【００２６】図５はクレジットカード会社側装置４００の内部構成を示す。クレジットカード会社側装置４００は、署名検証装置４０１、メモリ４０２、を備えている。

【００２７】図６は運搬者側装置５００の内部構成を示す。運搬者側装置５００は、メモリ５０１、通信装置５０２、暗復号化装置（共通鍵暗号）５０３、を備えている。

【００２８】図７は、運搬者携帯装置６００の内部構成を示す。運搬者携帯装置６００は、クレジットカード読み取り装置６０１、ハッシュ計算装置６０２、署名検証装置６０３、メモリ６０４、通信装置６０５、表示装置６０６、を備えている。

【００２９】買手は、クレジットカード１００による代金精算を前提として小売店側装置３００に商品発注を行い、運搬者を介して商品が買手のもとに配送される。

【００３０】（実施の形態１）買手は商品発注時と商品受け取り時に認証情報を作成し、クレジットカード会社はそれらの正当性を認証した後、買手の銀行口座から代金を引き落とす。本実施の形態では、このような場合について以下に詳しく述べる。また、本実施の形態では、公開鍵暗号にＲＳＡ（前述の「暗号理論入門」の第８８～９１頁参照）を用いる。

【００３１】買手はクレジットカード会社が発行したクレジットカード１００を所持する。クレジットカード１００内のメモリ１０１には買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が格納されている。クレジットカード会社はクレジットカード側装置４００内のメモリ４０２に買手の公開鍵（ｅ，ｎ）を保管している。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ≡１（ｍｏｄ　Ｎ）（Ｎはｐ－１とｑ－１の最小公倍数）。ｅｄ≡１（ｍｏｄ　Ｎ）は、ｅｄ－１がＮで割り切れることを意味する。

【００３２】図８を参照しながら、本実施の形態におけるショッピングの流れを説明する。

【００３３】（１）買手は購入を希望する商品を選び、買手側装置２００内の文書作成装置２０２を用いて注文書Ｐ（買手のＩＤ情報を含む）を作成する（８１）。注文書は、各小売店が定めるものであり、通常、買物注文の日付、注文商品とその個数、合計金額、クレジットカード会社名、クレジットカード番号、クレジットカードの有効期限等を記載したものである。さらに、買手はクレジットカード１００を買手側装置２００のクレジットカード読み取り装置２０１に接続する。買手側装置２００はハッシュ計算装置２０３を用いて注文書Ｐのハッシュ値ｈ（Ｐ）を計算し、クレジットカード１００のメモリ１０１に出力する。クレジットカード１００内は、メモリ１０１にある秘密鍵ｄと署名作成装置１０２を用いてクレジットカード１００内部にて、注文書Ｐに対する署名文Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成する（８２）。この式は、Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎは、ｅｘｐ（ｈ（Ｐ），ｄ）をｎで割った余りをＳ１とする、という意味である。ただし、ｈは公開されたハッシュ関数で、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表す。本例ではデジタル署名にＲＳＡを用いているので、ハッシュ値ｈ（Ｐ）は、０≦ｈ（Ｐ）≦ｎであればよい。クレジットカード１００は、署名文Ｓ１を買手側装置２００に出力する。買手側装置通信装置２０６を用いて注文書Ｐおよび署名文Ｓ１を小売店側装置３００に通信ネットワーク８００を介して送る（８３）。なお、安全性の観点からｎには５１２ビット以上の値が推奨される。

【００３４】（２）小売店は、注文書Ｐおよび署名文Ｓ１を受け取ると、注文書Ｐに記載の買手のＩＤ情報を用いて、クレジットカード会社側装置４００のメモリ４０２に格納されている買手の公開鍵（ｅ，ｎ）を問い合わせる（８４）。クレジット会社側装置４００は、これに応答して公開鍵を返送する（８５）。小売店側装置３００は、公開鍵（ｅ，ｎ）を受け取り、ハッシュ計算装置３０１と署名検証装置３０２を用いて、

ｈ（Ｐ）≡ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

の成立を確かめる（８６）。この式は、ｈ（Ｐ）－ｅｘｐ（Ｓ１，ｅ）がｎで割り切れることを意味する。これにより、署名文Ｓ１の認証を行う。

【００３５】（３）小売店は、買手の注文した商品の発送を運搬者を通して行う（８７）。また、代金の請求をクレジットカード会社に対して行う（８８）。この際、注文書Ｐと署名文Ｓ１をクレジットカード会社へ送信する。

【００３６】（４）買手は運搬者からの商品受け渡し時に、クレジットカード１００を運搬者が携帯する運搬者携帯装置６００のクレジットカード読み取り装置６０１に接続する。運搬者携帯装置６００はハッシュ計算装置６０２を用いて商品受取書Ｒのハッシュ値ｈ（Ｒ）を計算し、クレジットカード１００に出力する（９０）。商品受取書Ｒは、通常、運送業者が定めるものであり、発注者の名称、受取者の名称、日付等が記載されたものである。商品受取書Ｒは、通常、運搬者が小売店から商品発送を請け負った後に作成する。但し、小売店が作成

し、運搬者に商品発送を行った際に運搬車に渡すようにすることも可能である。クレジットカード１００はメモリ１０１に格納された秘密鍵ｄと署名作成装置１０２を用いて商品受取書Ｒに署名文Ｓ２をクレジットカード１００内部で、

Ｓ２＝ｅｘｐ（ｈ（Ｒ），ｄ）　ｍｏｄ　ｎ，

にて作成し、署名文Ｓ２と公開鍵（ｅ，ｎ）を運搬者携帯装置６００のメモリ６０４に出力する（９０）。このとき、受取書Ｒおよび署名Ｓ２のコピーをクレジットカード１００または他の記憶媒体に出力し、買手はこれを保管する、（５）運搬者携帯装置６００は、署名検証装置６０３を用いて、

ｈ（Ｒ）≡ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより、署名文Ｓ２の認証を行った後、Ｓ２を運搬者側装置５００のメモリ５０１に出力する（９１）。運搬者側装置５００は通信装置５０２を用いて通信ネットワーク８００を介してＲとＳ２をクレジットカード会社側装置４００に送信する（９２）。

【００３７】（６）クレジットカード会社側装置４００は、メモリ４０２に保管された買手の公開鍵（ｅ，ｎ）と署名検証装置４０１を用いて、

ｈ（Ｐ）≡ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

ｈ（Ｒ）≡ｅｘｐ（Ｓ２，ｅ）（ｍｏｄ　ｎ），

を確かめることにより、Ｓ１とＳ２の認証を行なう（９３）。その後、商品受取書Ｒの日付情報から商品返品有効期間を経た後、クレジットカード会社は買手の銀行口座から商品の代金を引き落とす（９４）。

【００３８】以上、一般的な変数により説明したが、きわめて簡略化したＲＳＡの一例を次に挙げる。

【００３９】公開鍵：ｎ＝５５，ｅ＝７

秘密鍵：ｐ＝５，ｑ＝１１，ｄ＝２３，７×２３＝１（ｍｏｄ　ｌｃｍ（ｐ－１，ｑ－１）＝２０），

ここに、ｌｃｍは最小公倍数を表す。

【００４０】平文：Ｍ＝３

暗号化：Ｃ＝ｅｘｐ（Ｍ，ｅ）　ｍｏｄ　ｎ，

ｅｘｐ（Ｍ，ｅ）＝３の７乗、ｎ＝５５なので、Ｃ＝４２となる。

【００４１】

復号化：Ｍ＝ｅｘｐ（Ｃ，ｄ）　ｍｏｄ　ｎ，

ｅｘｐ（Ｃ，ｄ）＝４２の２３乗、ｎ＝５５なので、Ｍ＝３となる。

【００４２】（実施の形態２）本実施の形態では、運送者は買手の注文商品の運搬状況の情報を信頼できるサーバに登録する。このような場合について、以下に詳しく述べる。また、本実施の形態においても、公開鍵暗号にＲＳＡを用いる。

【００４３】買手はクレジットカード会社が発行したクレジットカード１００を所持し、クレジットカード１００内のメモリ１０１には買手固有の秘密鍵ｄと公開鍵（ｅ，ｎ）が格納されており、クレジットカード会社はクレジットカード側装置４００内のメモリ４０２に買手の公開鍵（ｅ，ｎ）を保管している。ただし、ｎ＝ｐｑ（ｐ，ｑは素数），ｅｄ≡１（ｍｏｄ　Ｎ）（Ｎはｐ－１とｑ－１の最小公倍数）。

【００４４】（１）買手は購入を希望する商品を選び、買手側装置２００内の文書作成装置２０２を用いて注文書Ｐ（買手のＩＤ情報を含む）を作成する。さらに、買手はクレジットカード１００を買手側装置のクレジットカード読み取り装置２０１に接続する。買手側装置２００はハッシュ計算装置２０３を用いて注文書Ｐのハッシュ値ｈ（Ｐ）を計算し、クレジットカード１００に出力する。クレジットカード１００内はメモリ１０１にある秘密鍵ｄと署名作成装置１０２を用いてクレジットカード１００内部にて、注文書Ｐに対する署名文Ｓ１を、

Ｓ１＝ｅｘｐ（ｈ（Ｐ），ｄ）　ｍｏｄ　ｎ，

にて作成する。クレジットカード１００は、署名文Ｓ１を買手側装置２００に出力し、通信装置２０６を用いて注文書Ｐおよび署名文Ｓ１を小売店側装置３００に通信ネットワーク８００を介して送る。ただし、ｈは公開されたハッシュ関数で、ｅｘｐ（ａ，ｘ）はａをｘ乗した値を表す。

【００４５】（２）小売店は、注文書Ｐに記載の買手のＩＤ情報を用いて、クレジットカード会社側装置４００のメモリ４０２に格納されている買手の公開鍵（ｅ，ｎ）を問い合わせる。小売店側装置３００は、ハッシュ計算装置３０１と署名検証装置３０２を用いて、

ｈ（Ｐ）≡ｅｘｐ（Ｓ１，ｅ）（ｍｏｄ　ｎ），

を確かめることにより、署名文Ｓ１の認証を行う。

【００４６】（３）小売店は買手の注文商品に対してＩＤ番号Ｉを付け、さらに鍵生成装置３０４を用いて固有の鍵情報Ｋ（共通鍵暗号の鍵）を作成する。小売店側装置３００は暗復号化装置３０３を用いて鍵Ｋを買手の公開鍵（ｅ，ｎ）から、

Ｗ＝ｅｘｐ（Ｋ，ｅ）　ｍｏｄ　ｎ，

にて暗号化して、通信装置３０５を用いてＩとＷを通信ネットワーク８００を介して買手側装置２００に送る。さらに小売店は買手が注文した商品とＩＤ番号Ｉと鍵Ｋを運送業者に渡し、代金の請求をクレジットカード会社に対して行う。

【００４７】（４）運送業者は商品の運搬状況（商品がどこにあって、いつ買手の手元に到着するか等）を示す運搬状況の情報Ｓを逐次、運搬者側装置５００内の暗復号化装置５０３を用いてＳを鍵Ｋで暗号化する。すなわち、暗号文

Ｅ（Ｓ）＝Ｅ（Ｓ：Ｋ），

を計算して、通信装置５０２を用いて通信ネットワーク８００を介して信頼できるサーバ７００にＳを登録する。なお、共通鍵暗号方式としては、ＤＥＳ，ＦＥＡＬ等の公知のものを用いることができる。

【００４８】（４）買手はクレジットカード１００を買

手側装置２００のクレジットカード読み取り装置２０１に接続し、Ｗをクレジットカード１００に出力し、メモリ１０１内の秘密鍵ｄと暗復号化装置１０３を用いて、

Ｋ＝ｅｘｐ（Ｗ，ｄ）　ｍｏｄ　ｎ，

にて、鍵Ｋを復号化し、買手側装置２００のメモリ２０５に出力する。買手は、買手の注文した商品の運搬状況を知ることを目的に買手側装置２００内の通信装置２０６を用いてサーバ７００にアクセスし、商品の識別情報Ｉから暗号化データＥ（Ｓ）を検索し、Ｅ（Ｓ）をメモリ２０５に格納する。買手側装置２００は鍵Ｋと暗復号化装置２０４を用いて、

Ｓ＝Ｄ（Ｅ：Ｋ），

にて、Ｓを復号化する。

【００４９】（実施の形態３）実施の形態１において、運搬者携帯装置６００は文書を表示する表示装置６０６を備えており、買手は表示装置６０６に表示された商品受取書を視覚にて確認し、クレジットカード１００を運搬者携帯装置６００のクレジットカード読み取り装置６０１に接続し、実施の形態１の方法により署名を行う。さらに、運搬者携帯装置６００は表示装置６０６に該署名の正否を表示する。表示装置６０６の画面に表示する内容としては、運搬内容、受取者名、差出名、運搬者名、受取日付、署名（済または未済）等が考えられる。署名の項目は、署名の正当性が確認されると「済」が表示される。

【００５０】

【発明の効果】本発明によれば、買手はクレジットカードによる代金支払いを前提として、通信ネットワークを介して小売店に対して商品注文を行い、小売店は買手の注文商品を運搬者に委託して発送し、クレジットカード会社は買手の銀行口座より商品代金を引き落とす電子ショッピングシステムにおいて、クレジットカード会社は、買手の商品注文時のデジタル署名と商品受け取り時のデジタル署名の双方の正当性を確認した後、代金引き落としを行うため、不正な小売店が買手からクレジットカードの情報を引き出し、商品を買手に渡すことなく代金を得る不正を防止することができる。また、商品の運搬状況の情報を買い手、小売店、および運搬者以外のものが知ることのできない鍵で暗号化してサーバに格納することにより、買手のプライバシーを保護しながら、買手は自分の発注した商品が買手の手元に届くまでの運送状況の情報を安全に知ることができる。

【図面の簡単な説明】

【図１】本発明のシステム構成を示す図である。

【図２】図１のシステム構成内のクレジットカードの内部構成を示す図である。

【図３】図１のシステム構成内の買手側装置の内部構成を示す図である。

【図４】図１のシステム構成内の小売店側装置の内部構成を示す図である。

【図５】図１のシステム構成内のクレジットカード会社の内部構成を示す図である。

【図６】図１のシステム構成内の運搬者側装置の内部構成を示す図である。

【図７】図１のシステム構成内の運搬者携帯装置の内部構成を示す図である。

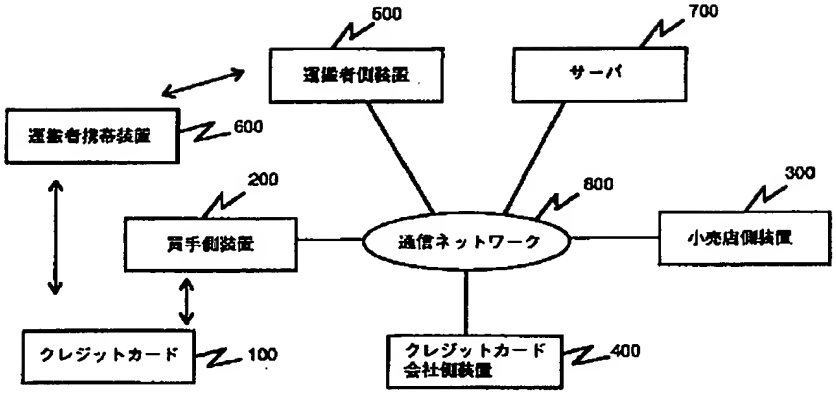
【図８】図１のシステム構成におけるショッピングの流れを示す図である。

【符号の説明】

１００…クレジットカード、１０１…クレジットカード１００内のメモリ、１０２…クレジットカード１００内の署名作成装置、１０３…クレジットカード１００内の暗復号化装置（公開鍵暗号）、２００…買手側装置、２０１…買手側装置２００内のクレジットカード読み取り装置、２０２…買手側装置２００内の文書作成装置、２０３…買手側装置２００内のハッシュ計算装置、２０４…買手側装置２００内の暗復号化装置（共通鍵暗号）、２０５…買手側装置２００内のメモリ、２０６…買手側装置２００内の通信装置、３００…小売店側装置、３０１…小売店側装置３００内のハッシュ計算装置、３０２…小売店側装置３００内の署名検証装置、３０３…小売店側装置３００内の暗復号化装置（公開鍵暗号）、３０４…小売店側装置３００内の鍵生成装置、３０５…小売店側装置３００内の通信装置、４００…クレジットカード会社側装置、４０１…クレジットカード会社側装置４００内の署名検証装置、４０２…クレジットカード会社側装置４００内のメモリ、５００…運搬者側装置、５０１…運搬者側装置５００内のメモリ、５０２…運搬者側装置５００内の通信装置、５０３…運搬者側装置５００内の暗復号化装置（共通鍵暗号）、６００…運搬者携帯装置、６０１…運搬者携帯装置６００内のクレジットカード読み取り装置、６０２…運搬者携帯装置６００内のハッシュ計算装置、６０３…運搬者携帯装置６００内の署名検証装置、６０４…運搬者携帯装置６００内のメモリ、６０５…運搬者携帯装置６００内の通信装置、６０６…運搬者携帯装置６００内の表示装置、７００…サーバ、８００…通信ネットワーク。

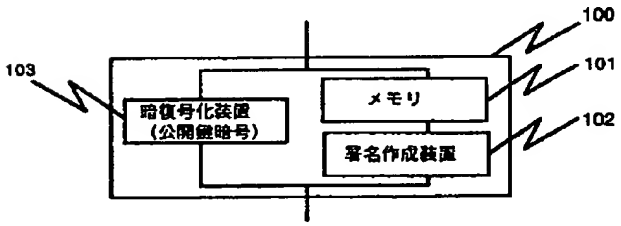
【図１】

システム構成（図１）



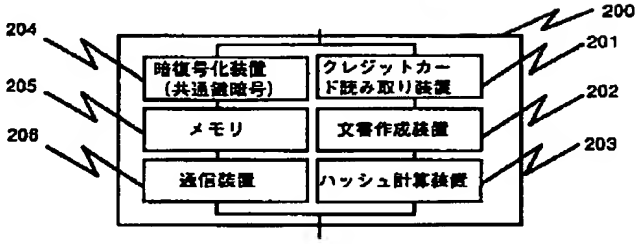
【図２】

クレジットカード内部構成（図２）



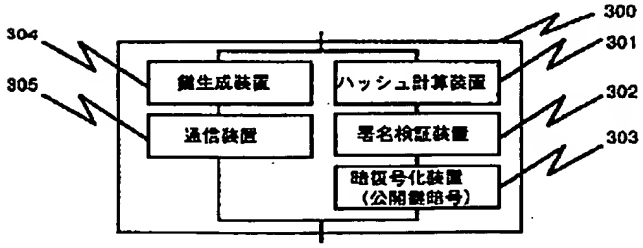
【図３】

買手側装置内部構成（図３）



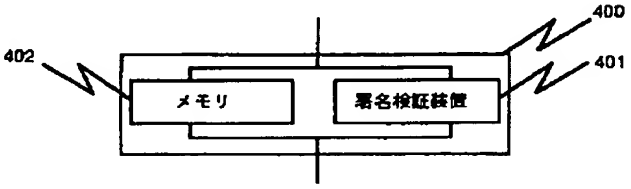
【図４】

小売店側装置内部構成（図４）



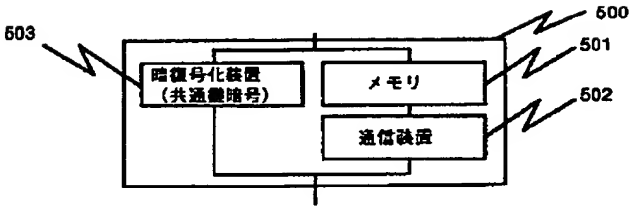
【図５】

クレジットカード会社側装置内部構成（図５）



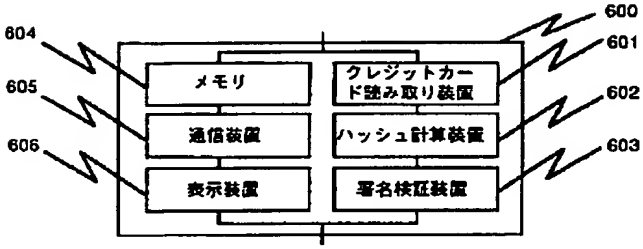
【図６】

運搬者側装置内部構成（図６）



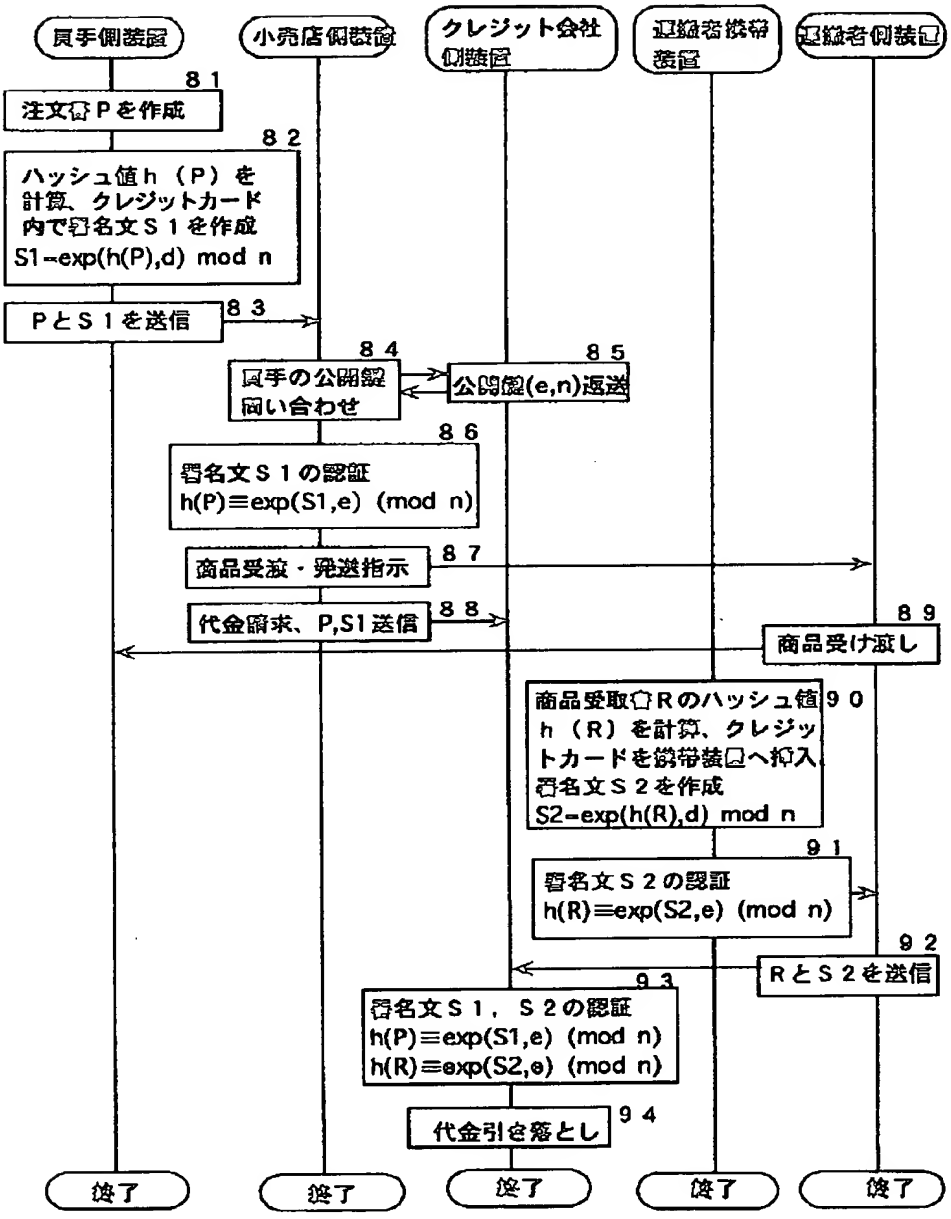
【図７】

運搬者携帯装置内部構成（図７）



【図８】

図８



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
			Ｈ０４Ｌ　9/00	６７５Ｂ

(72)発明者　梅木　久志
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　花岡　かほる
神奈川県川崎市幸区鹿島田890番地の12
株式会社日立製作所情報システム事業部内